Cassandra Crossing/ Zombie nella Rete

(350)—L'organizzazione che manovrava la botnet Conficker èstata smantellata da anni ma le macchine infette che sono ancora pronte ad…

Cassandra Crossing/ Zombie nella Rete

Figure 1:

(350)—L'organizzazione che manovrava la botnet Conficker èstata smantellata da anni ma le macchine infette che sono ancora pronte ad accogliere ordini sono un milione. Un piccolo esercito nella Internet delle Cose Abbandonate.

14 agosto 2015—Per tanti anni la letteratura Cyberpunk e Steampunk ci hanno abituato a ritenere del tutto naturale l'esistenza di persone strane o pericolose, di cose strane e pericolose e di software strani o pericolosi nella Rete.

L'*affaire* Silk Road ha, per le persone che negli ultimi 10 anni avessero fatto un viaggio interplanetario, aperto gli occhi a molti di coloro che ancora ignoravano come la Rete avesse grossomodo la stessa percentuale di imbecilli e criminali del resto dell'universo.

Ed onore deve essere fatto a chi, spronato dalla figura di Invernomuto, ha con grande perseveranza lavorato nel campo dell'intelligenza artificiale negli ultimi 30 anni.

Ma le mai arrivate A.I. erano attese come "persone", mentre l'Internet delle Cose, in cui ci siamo improvvisamente trovati immersi, è stranamente giunta assai inaspettata.

Ed oltre a creare le condizioni per un ampliamento esplosivo della Rete in termini di pervasività e di insicurezza, ha creato le opportunità per una Rete "differenziata", non per i suoi utenti, ma per i suoi "abitanti".

Ha creato “bassifondi” nella Rete, nicchie di cui forse gli ecologi piuttosto che gli informatici dovrebbero occuparsi.

Un freschissimo contributo che verrà presentato oggi ad USENIX e già reperibile in Rete, dal titolo Post-Mortem of a Zombie: Conficker Cleanup After Six Years, non solo disserta ma racconta la nascita di una famosa botnet, la guerra che le è stata scatenata contro e l’imprevisto finale alla Silent Running... solo non sereno, al contrario inquietante.

Ma andiamo con ordine, iniziando con un avvertimento.

Lo scopo del paper citato è principalmente quello di elaborare e validare un modello statistico della diffusione della botnet Conficker, perché di essa esiste un enorme database di monitoraggio che copre addirittura un arco di 6 anni (Conficker è del 2009) la sua parte centrale non è quindi ben leggibile a chi non mastica statistica.

Ma dal punto di vista di Cassandra e dei suoi intrepidi 24 lettori sono invece importanti la cronologia, i fatti, le conclusioni.

La conclusione più importante è che dopo la neutralizzazione dell’organizzazione che ha creato e gestito Conficker e la sua evoluzione, e la successiva distruzione dei centri di Comando & Controllo, Conficker, per essere morta, gode ancora di una salute invidiabile.Le macchine infette che ancora cercano di collegarsi agli ormai estinti centri di C&C, e che vengono per questo loggate a livello di IP sul database di monitoraggio, sono un milione.

Un milione di abitanti della Rete, che vivono e ancora si riproducono malgrado siano stati abbandonati dei loro “padroni”. Abitanti il cui numero è continuato ad aumentare anche dopo la decapitazione della botnet e la distribuzione della patch della vulnerabilità di base.

Un milione di longevi abitanti il cui tasso di descrescita è bassissimo, e che sembrano destinati a durare malgrado gli aggiornamenti dei sistemi operativi, la sostituzione dei computer guasti ed altro.

Un milione di *confickeriani* che sono già in compagnia di altre popolazioni simili orfane di altri malware.

Allontaniamoci ora definitivamente dal “sentiero” tracciato dal paper, che trae comunque alcune conclusioni a riguardo, e proseguiamo con un approccio “ecologico”.

C’è in Rete una nicchia ecologica che è stata occupata dagli inattesi orfani di Conficker. Le normali operazioni di lotta alla botnet durate per anni, in alcuni paesi anche con il coinvolgimento di organismi appositi e la cooperazione degli ISP, non l’hanno affatto distrutta.

Cosa costituisce questa nicchia?Forse server fax basati su XP o 98, accesi da anni e che svolgono normalmente il loro lavoro.

O magari moderni frigoriferi intelligenti che mai nessuno aggiornerà

O forse computer di villaggi africani, alimentati con una bicicletta e con un upstream satellitare.

O registratori di cassa in un suk tunisino.

O schede embedded in qualche centrale nucleare.

O computer fossili custoditi da Asbesto in quel di Palazzolo Acreide nel Museo dell’Informatica Funzionante.

O coniglietti resi molto più intelligenti mediante trapianto x86.O Arduini, interfacciati con schede pc in una macchina rovesciacalzini.

Probabilmente è l'inizio dell'Internet delle Cose Abbandonate, destinata a diventare un mar dei Sargassi digitale. Nessuna enumerazione quindi potrà mai essere esaustiva: è necessario un cambio di paradigma.Non più un parco macchine installato da disinfestare. Piuttosto un mondo che si sta evolvendo, in parte guidato ancora dagli esseri umani ma in parte autonomo, la cui autonomia è destinata a crescere.Un mondo in espansione.Un terreno di evoluzione e di conquista.

Un terreno dove adware abbandonati e cyberarmi sfuggite al controllo magari si confronteranno in una lotta senza quartiere: auguriamoci che non diventino mai Skynet.

Perché forse la prima intelligenza artificiale, buona, indifferente o cattiva che sia, si evolverà "naturalmente" non in laboratorio ma proprio qui.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on July 26, 2023.

Canonical link

Exported from Medium on August 27, 2025.